

**REMARKS**

Reconsideration and allowance of the subject application are respectfully requested.

Examiner rejects claims 31-45 under 35 U.S.C. §101 stating that these claims recite “a computer program product” which is not a tangible embodiment and requiring amendment to “tangibly embody these claims on a computer recordable medium.” These claims have been amended as requested. Withdrawal of the rejection under 35 U.S.C. §101 is respectfully requested.

The Examiner makes an obviousness-type double patenting rejection of all claims 1-45 contending that claims 1-36 of commonly-owned application serial number 10/003,265 (the ‘265 application) “contains every element of claims 1-45 of the instant application and as such anticipates claims 1-45 of the instant application.” Applicants respectfully traverse this rejection.

Claim 1 of the instant application is directed to “a load balancing device for balancing the load across a plurality of proxy devices.” By contrast, independent claim 1 of the ‘265 application only describes a “proxy device for performing malware scanning.” There is no recitation in claim 1 of the ‘265 application or any of its dependent claims of a load balancing device or of load balancing logic as recited in claim 1 of the instant application. Independent claim 11 of the ‘265 application relates to a balanced proxy system that includes “the load balancing devices claimed in claim 1.” Claim 16 recites a method of operating a load balancing device to balance the load across a plurality of proxy devices and recites applying a predetermined load balancing routine. Similar recitations are found in independent claims 31 and 40.

The claims of the co-pending application 10/003,265 are mainly directed to the proxy device for performing malware scanning and not to load balancing. Although claim 12 of the

'265 application recites a balanced proxy system, claim 12 specifically recites that the load balancing mechanism is a "passive load balancing mechanism" that ensures that "an access request issued by a particular client device will be directed to a predetermined one of said proxy devices dependent on how that client device was configured by the passive load balancing mechanism." This is a different load balancing mechanism/approach than that described in the claims of the instant application. Claim 12 of the '265 application does not recite, for example, "load balancing logic for applying a predetermined load balancing routine to determine to which proxy device to direct that access request." The same is true for claims 24 and 36 the '265 application--the only other claims to recite a passive load balancing mechanism as in claim 12. The other claims of the co-pending application make no mention of load balancing at all. Accordingly, the Applicants respectfully request that the double patenting rejection be withdrawn.

Claims 1-12, 16-27, and 31-42 remain rejected under 35 U.S.C. §112 as being unpatentable over Asai and Hailpern. This rejection is respectfully traversed.

Sections 6 to 24 of the current Office Action appear to be the same as in the first Office Action. So Applicants' response is now directed to the Examiner's comments about the arguments presented in the previous response.

In section 27 of the Office Action, it appears that the Examiner is initially relying on a typographical error in the response previously filed. Applicants apologize for this typographic error. But it is clear from the context of the prior response that Hailpern does not apply a predetermined load balancing routine in order to determine to which proxy device to direct the access request. See, for example, the introduction in the prior response to the claim distinctions relative to Hailpern: "Hailpern lacks a load balancing device arranged... to apply a

predetermined load balancing routine to determine to which proxy device to direct that access request.” The basis of Applicants’ arguments relative to Hailpern were clear in the context of the response, and the intended meaning was certainly understood by the Examiner, see e.g., “Furthermore Hailpern discloses...” from section 27 of the Office Action.

As admitted by the Examiner, Asai does not disclose that the proxy device (the context server of Fig. 1) performing malware scanning of files stored within the file storage device. Indeed, Asai does not even disclose malware scanning.

The Examiner relies on Hailpern in an attempt to remedy Asai's deficiencies. Hailpern describes a proxy server system arranged to perform malware scanning. Hailpern's client devices access via the Internet content stored on content servers. As is known in such systems, a client device typically accesses the Internet via a pre-defined sequence of proxy servers. For example, with reference to Figure 1, the client device 1220 accesses the Internet 1020 via the sequence of proxy servers 1140, 1110, and 1100. Hailpern enables the proxy servers in that pre-defined sequence to collaborate when performing virus checking based on meta-information associated with each data object retrieved via the Internet (column 1, lines 25-28). The meta-information enables any particular proxy server to keep track of processing performed by any other proxy server in the link between the client device and the Internet. As a result, those proxy servers can collaborate to perform virus checking.

Hailpern's teachings differ from what is recited in claim 1. In particular, in Hailpern, the sequence of proxy servers required to process an access request is predetermined dependent upon the client. What Hailpern provides is a mechanism for spreading out the required virus checking among those proxy servers in the sequence. In contrast, claim 1 recites a dedicated load balancing device that intercepts access requests issued to the file storage device in order to select

a particular proxy server in accordance with a balancing routine. There is clearly no such load balancing device described in Hailpern.

As a result, Hailpern also does not describe any of the other claim features of the load balancing device set out in claim 1. For example, Hailpern lacks “load balancing logic for applying a predetermined load balancing routine to determine to which proxy device to direct that access request.” In Hailpern, the sequence of proxy servers required to process any particular access request is predetermined, and hence, there is no determination to be made. Accordingly, it is also clear that Hailpern does not disclose a load balancing device with a “proxy device interface for sending the access request to the proxy device determined by the load balancing logic.”

From an architectural point of view, Asai is the more relevant reference employing a load distribution server 20 which the Examiner has considered equivalent to the claimed load balancing device. But Asai does not describe any malware scanning, and any malware scanning would be performed within Asai’s content server 30 in accordance with known techniques. In contrast, Hailpern is an entirely different system where any particular client device accesses file content over the Internet via a pre-ordained sequence of proxy servers. Within such a system, there is no role for the claimed load balancing device because there is no ability to choose between different proxy devices.

Turning to the Examiner’s comments at section 29 of the Official Action, the Examiner fails to explain how Asai could be adapted based on Hailpern. In which elements of Hailpern does the Examiner believe the teachings of Hailpern could be implemented? In Asai’s system, the load distribution server 20 chooses a single cache server to handle the access to the content

server 30, and hence, Hailpern's meta-information routed between proxy servers at different levels (see Fig. 1) would have no use.

The combination of Asai and Hailpern also fails to disclose the claimed feature of issuing "access request using a dedicated file access protocol." The Examiner simply identifies Asai's content server 30 but does not point out where Asai teaches an access request using a dedicated file access protocol. Moreover, the Examiner fails to point out where either reference teaches the specific examples of dedicated file access protocols, such as the server message block (SMB) protocol and the network file system (NFS) protocol recited in several dependent claims. Hailpern's Internet-based system means that the access request are issued using the HTTP protocol. See, for example, col. 9, lines 61-65. HTTP is not a dedicated file access protocol, but instead, is a protocol primarily designed for transmission of text.

Thus, the combination of Asai and Hailpern fails to disclose multiple features recited in the claims. Applicants also refer the Examiner to the earlier response in which it was demonstrated that neither Hailpern nor Asai are directed to the same problem as the instant inventors. Although not addressed by the Examiner, the Federal Circuit has clearly instructed that the consideration of the problem confronted by the inventors is required in determining whether it would be have been obvious to combine references in order to solve that problem. *Northern Telecom, Inc. v. Datapoint Corp.*, 908 F.2d 931, 935 (Fed. Cir. 1990). Lacking that same problem analysis, the obviousness rejections are also deficient because they fail to provide the requisite motivation to make the proposed combinations and modifications of Asai and Hailpern.

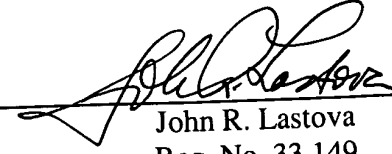
The application is in condition for allowance. An early notice to that effect is earnestly solicited.

WOLFF et al  
Appl. No. 10/004,120  
August 15, 2005

Respectfully submitted,

**NIXON & VANDERHYE P.C.**

By:

  
John R. Lastova  
Reg. No. 33,149

JRL:sd  
901 North Glebe Road, 11th Floor  
Arlington, VA 22203-1808  
Telephone: (703) 816-4000  
Facsimile: (703) 816-4100